Ciphers

- Mechanism that decides the process of encryption/decryption
- Stream Cipher: Bit-by-bit encryption / decryption
- Block Cipher: Block-by-block encryption / decryption

Types of Cipher

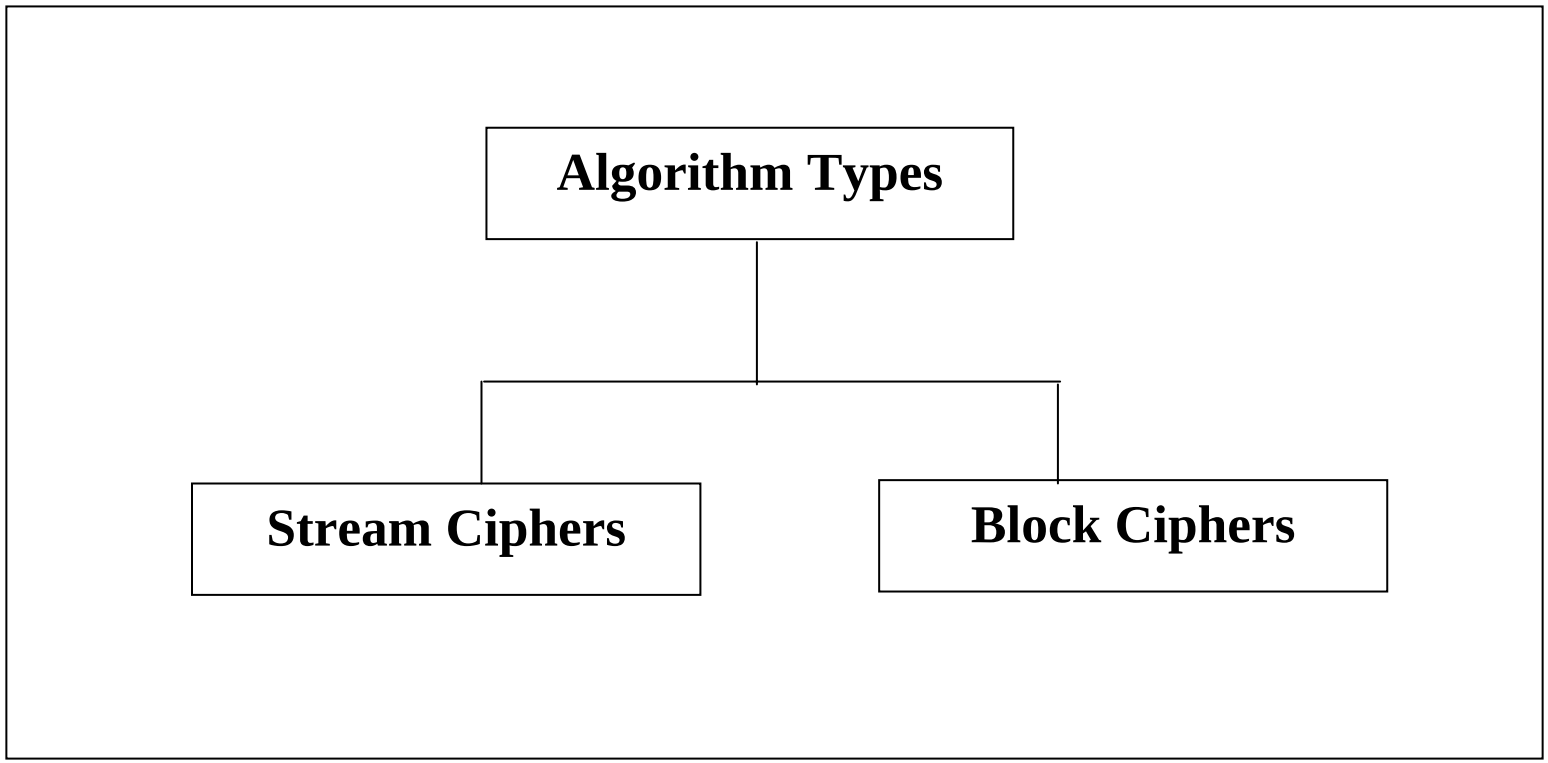

Fig 3.1

Stream Cipher Example

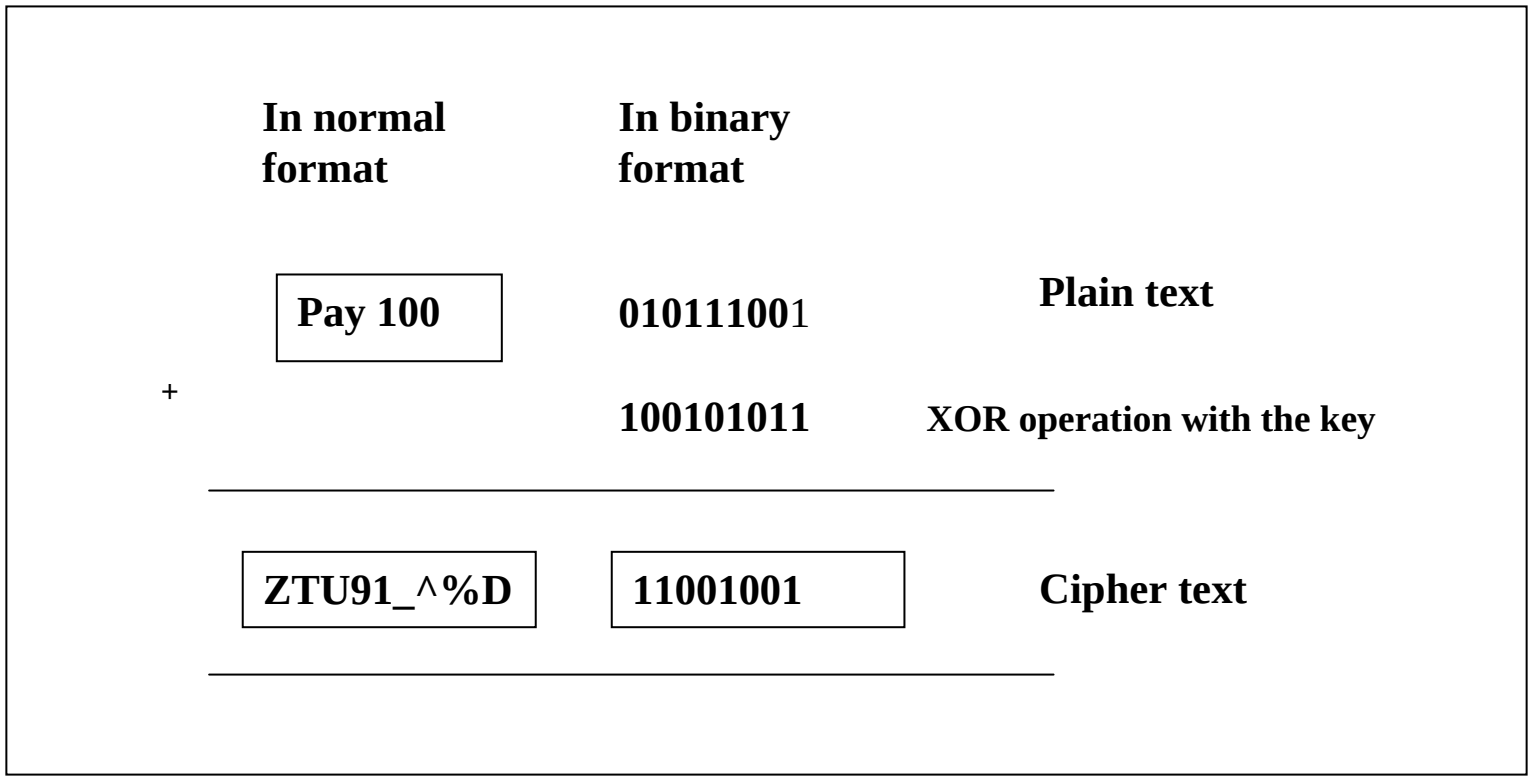

Fig 3.3

Block Cipher Example

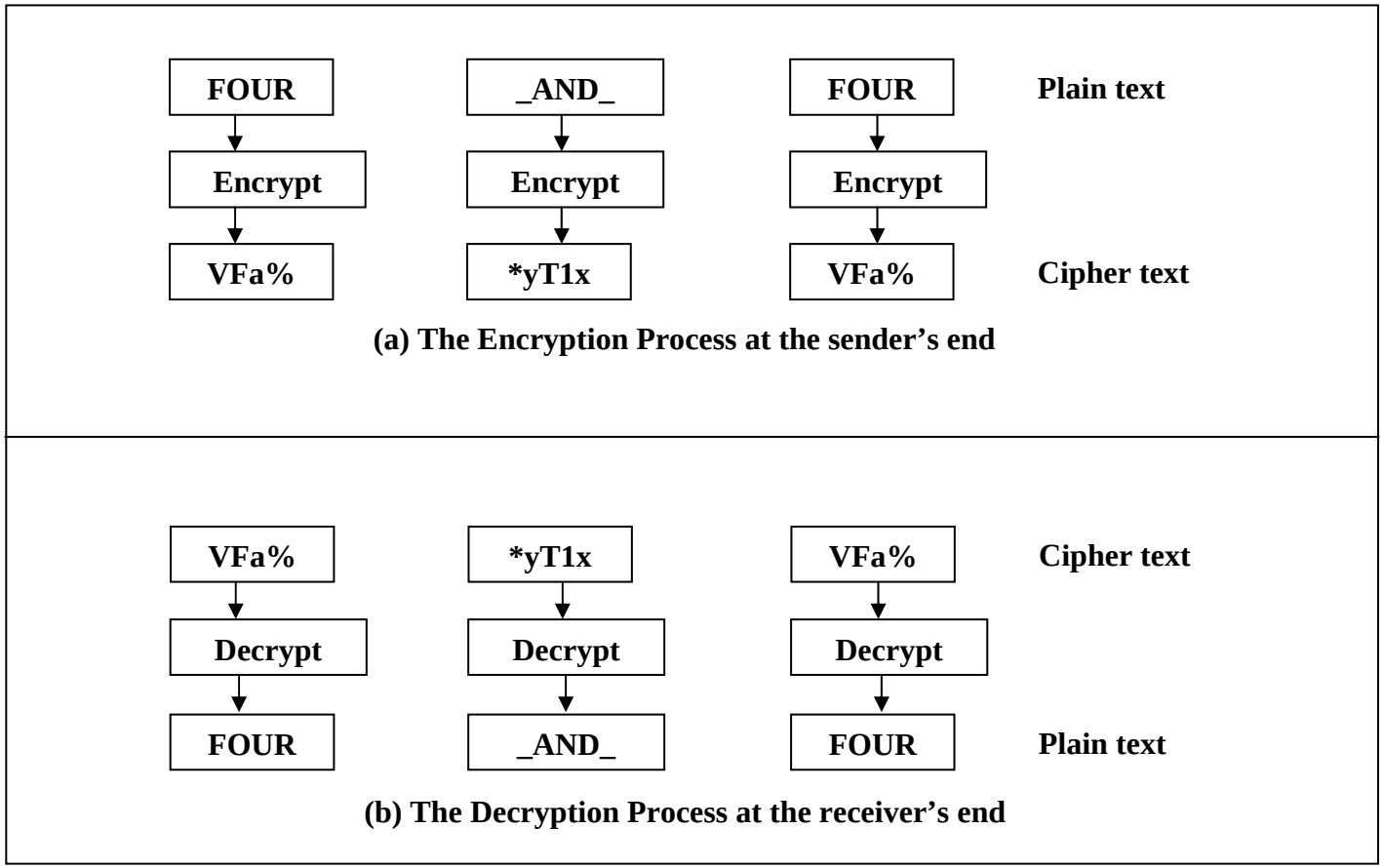

Fig 3.4

Algorithm Modes

- Add randomness to block cipher
- Otherwise, block cipher becomes predictable
- Four main modes

Algorithm Modes

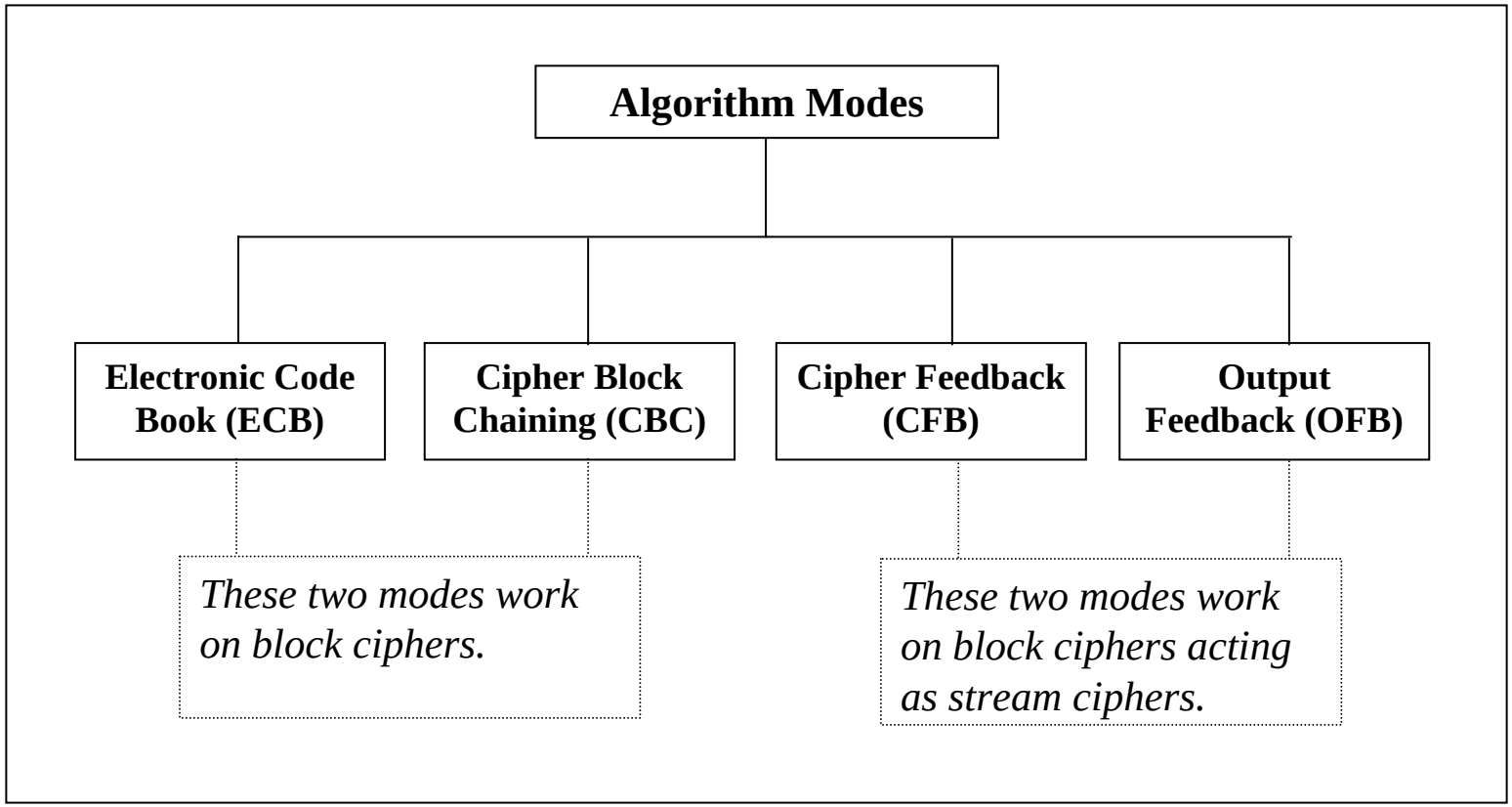

Fig 3.5

Encryption in ECB Mode

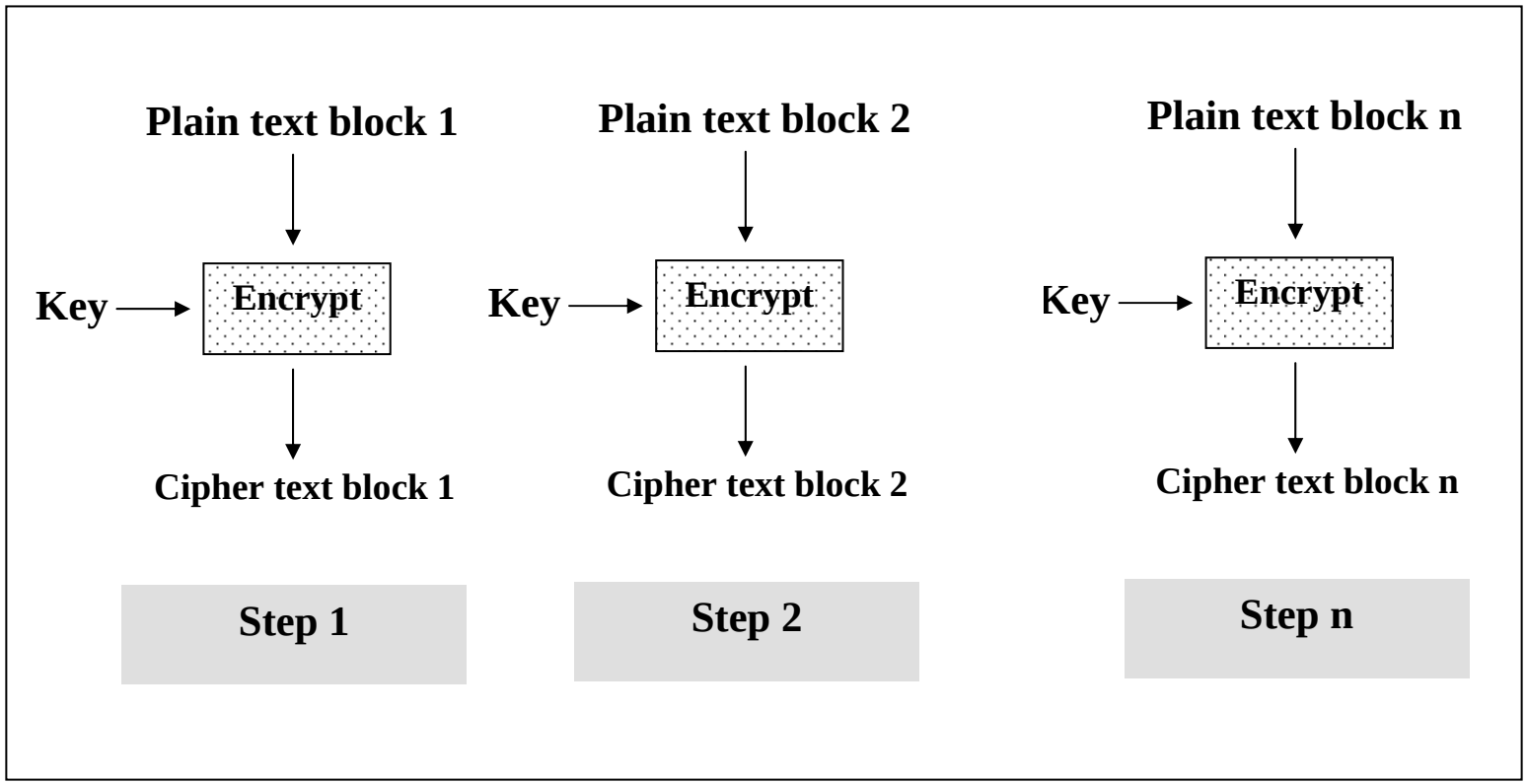

Fig 3.6

Decryption in ECB Mode

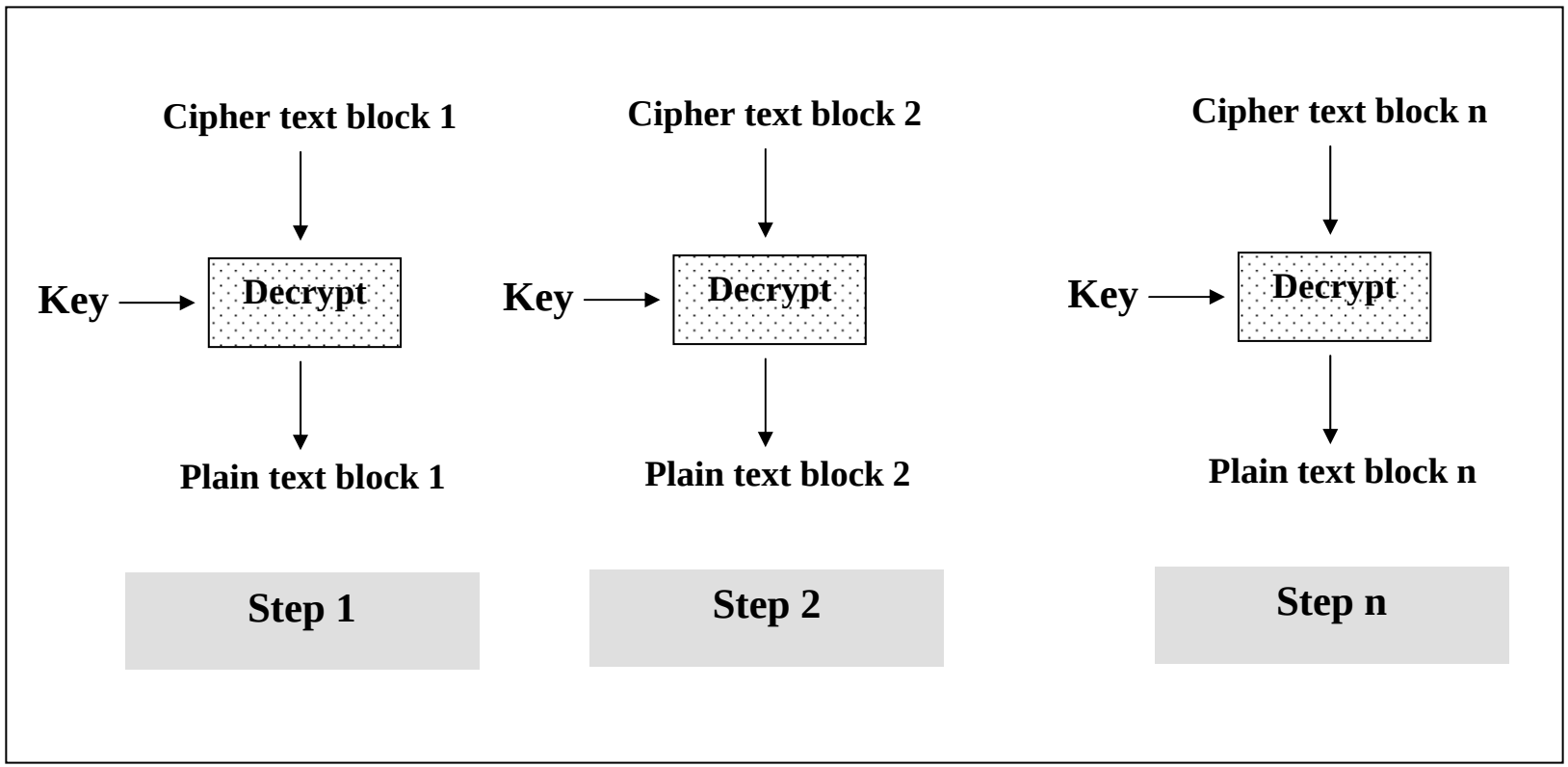

Fig 3.7

Encryption in CBC Mode

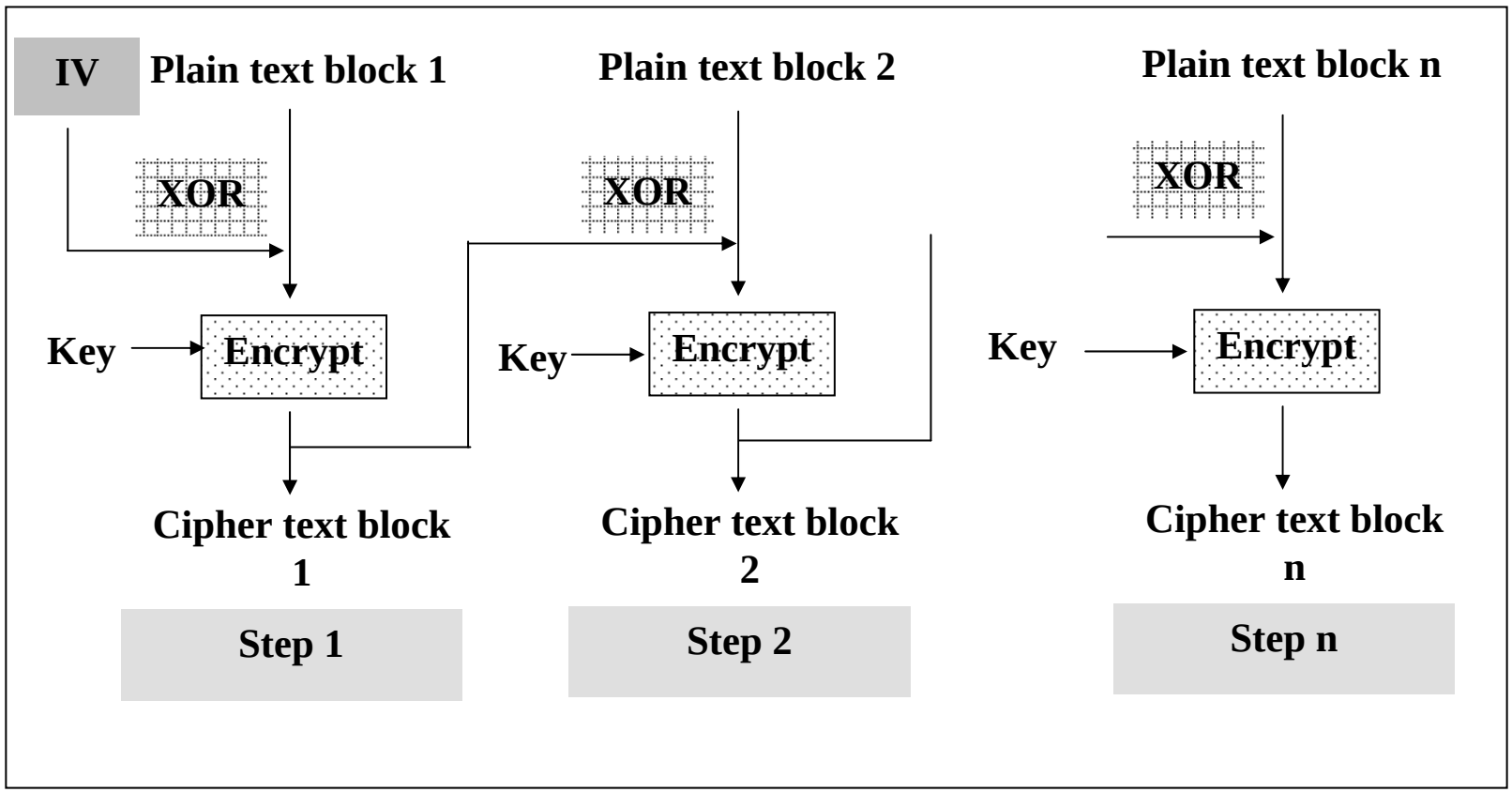

Fig 3.8

Decryption in CBC Mode

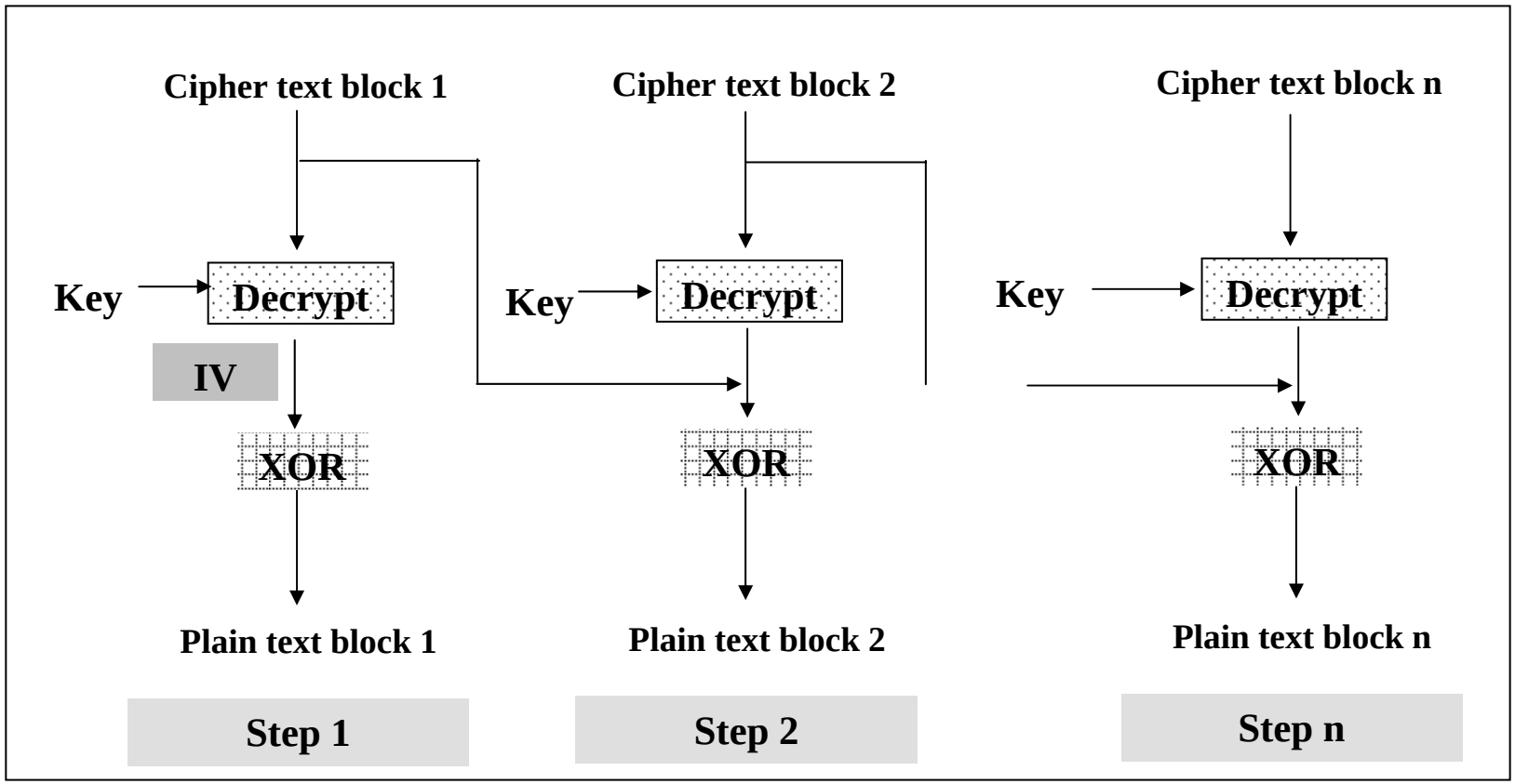

Fig 3.9

Encryption in CFB Mode

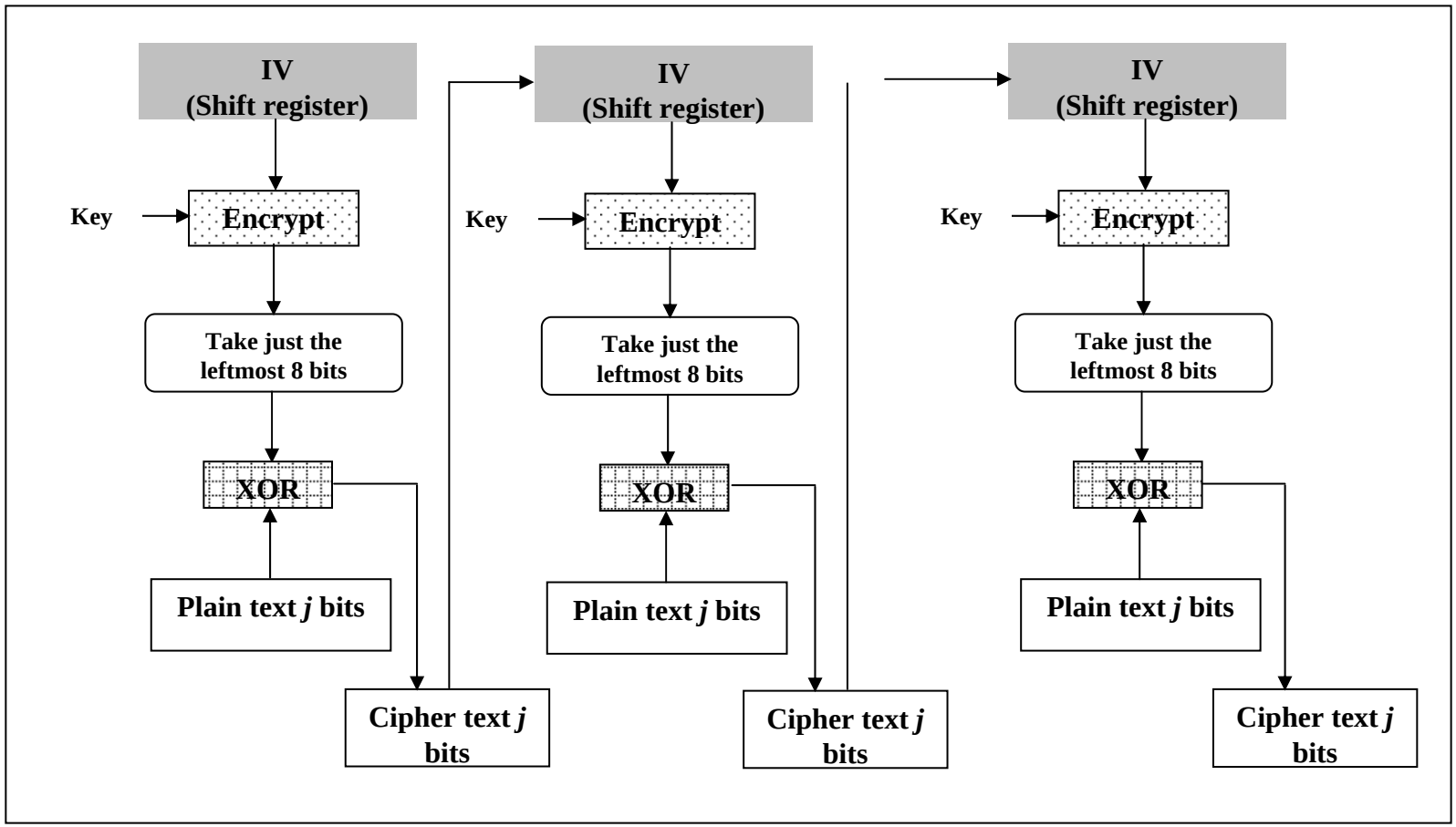

Fig 3.13

Encryption in OFB Mode

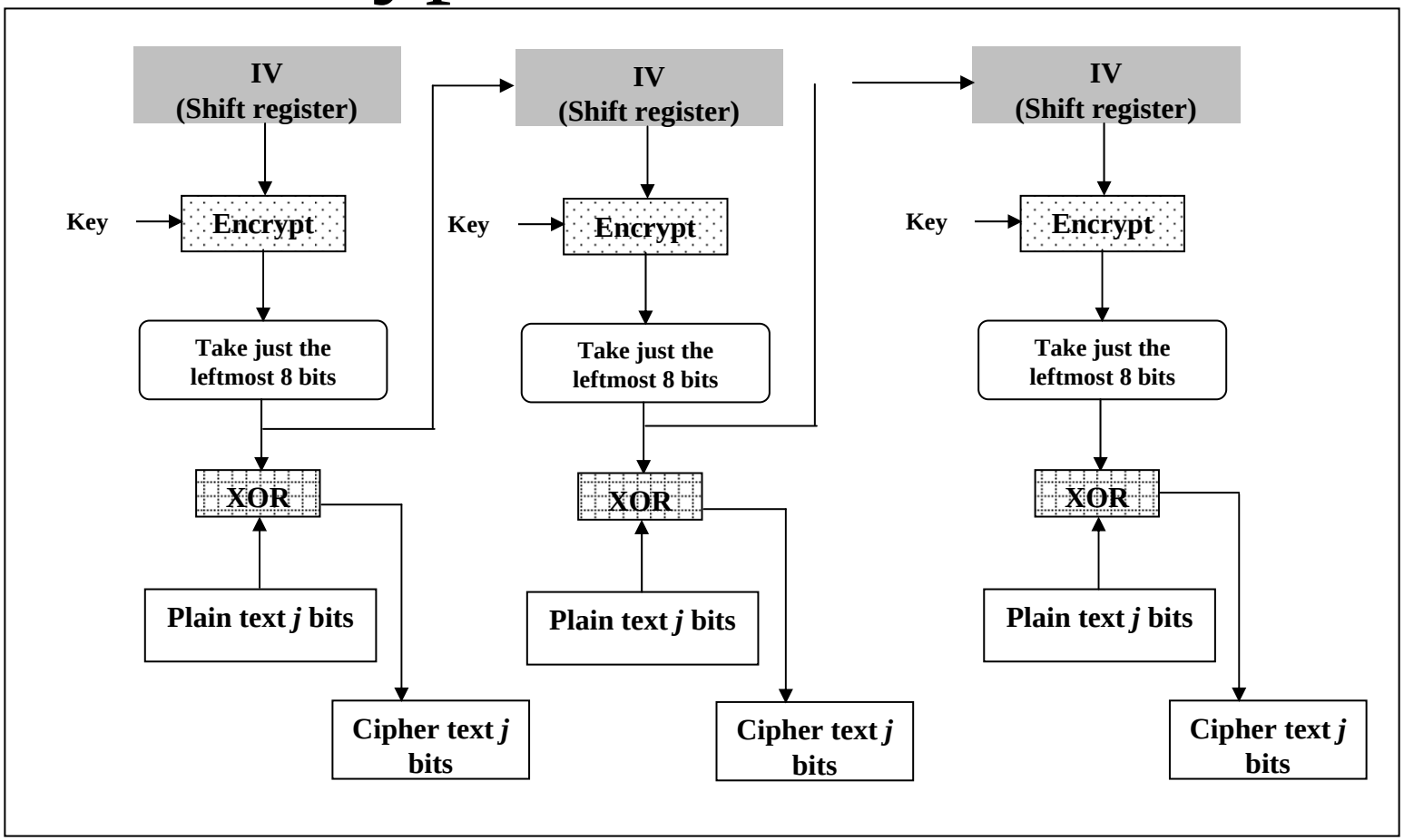

Fig 3.14

Symmetric Key Cryptography

- Same key used for encryption and decryption
- Examples: DES, IDEA, RC5, Blowfish, AES
- Quite popular and fast

Symmetric Key Cryptography

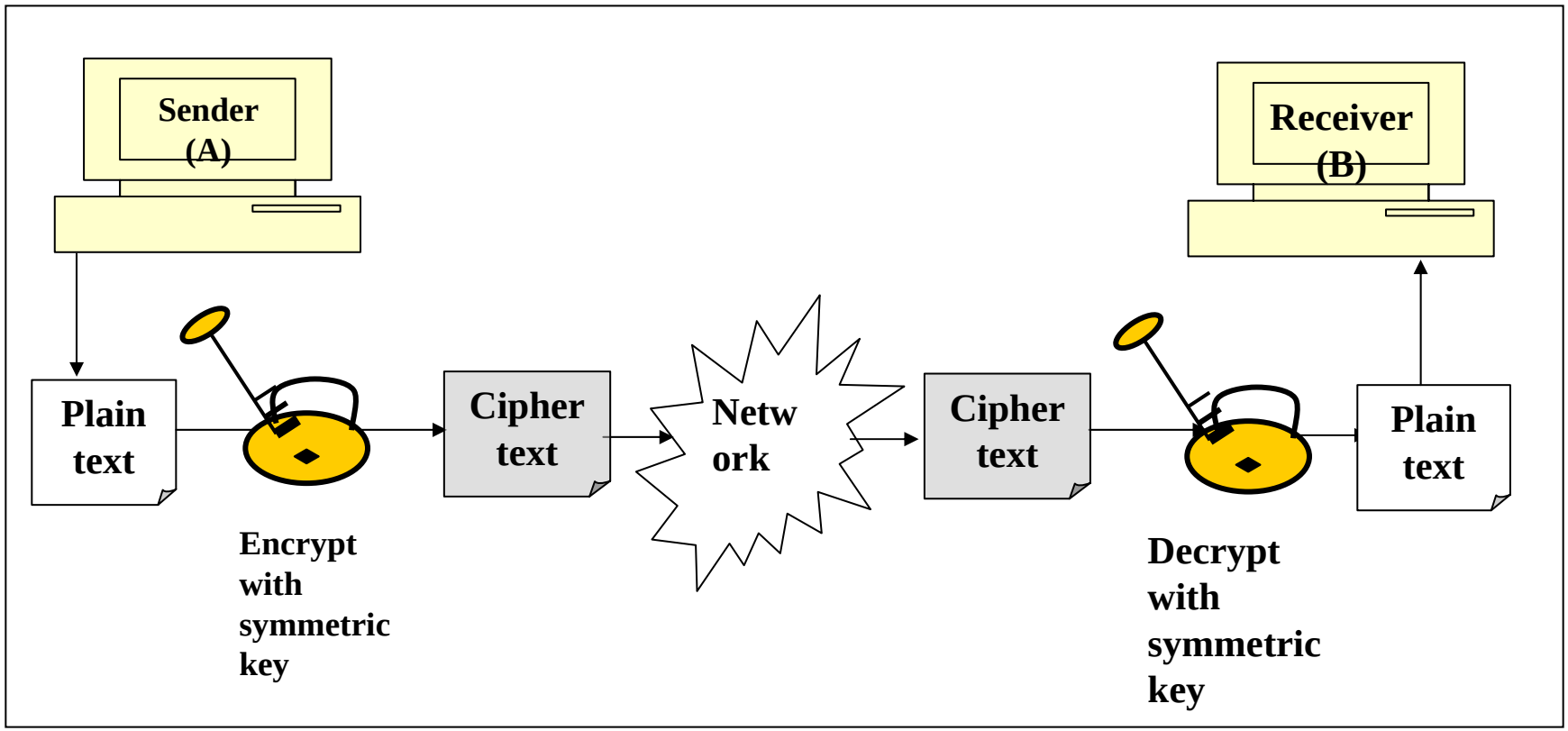

Fig 3.15

Conceptual View of DES

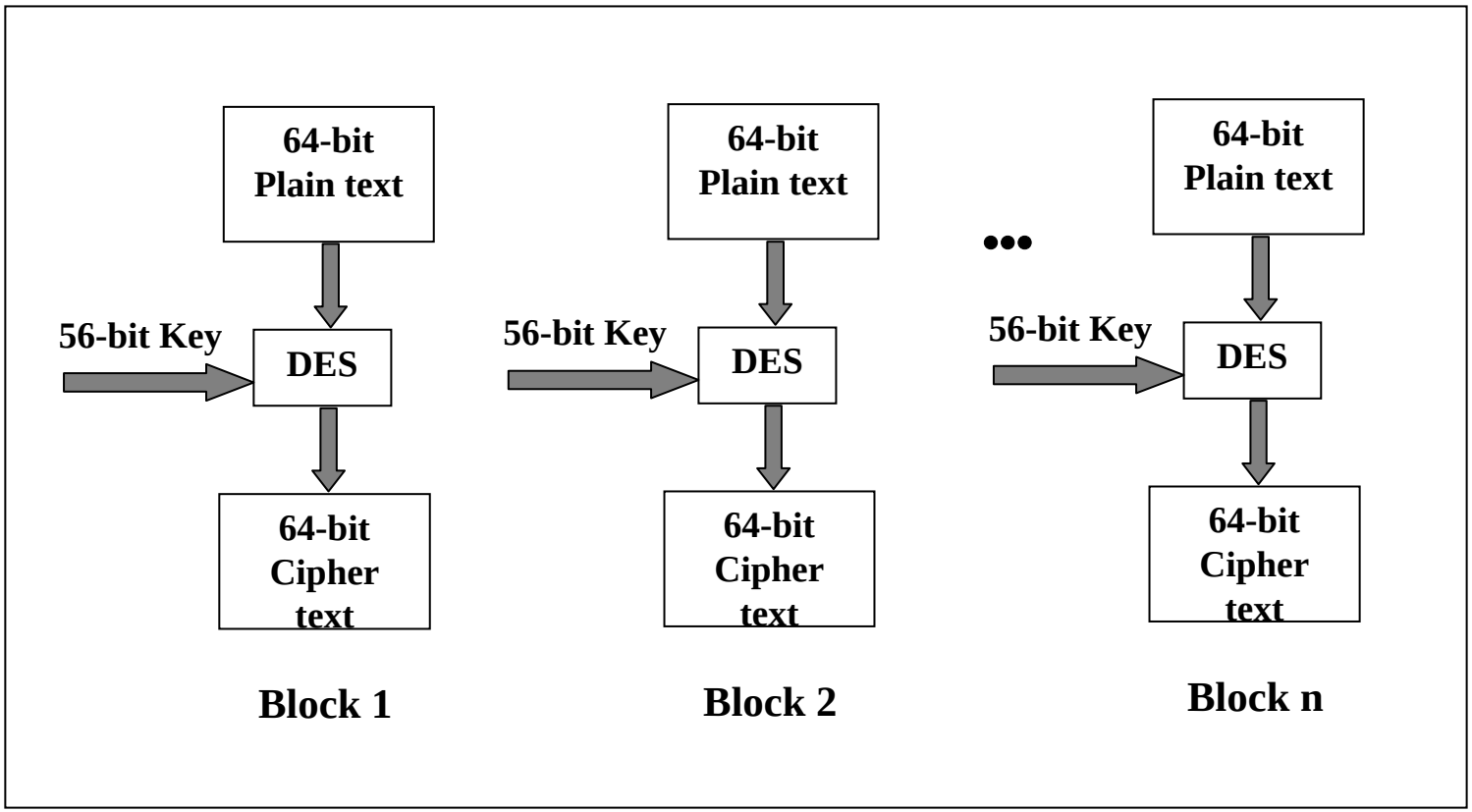

Fig 3.16

Broad Level Steps in DES

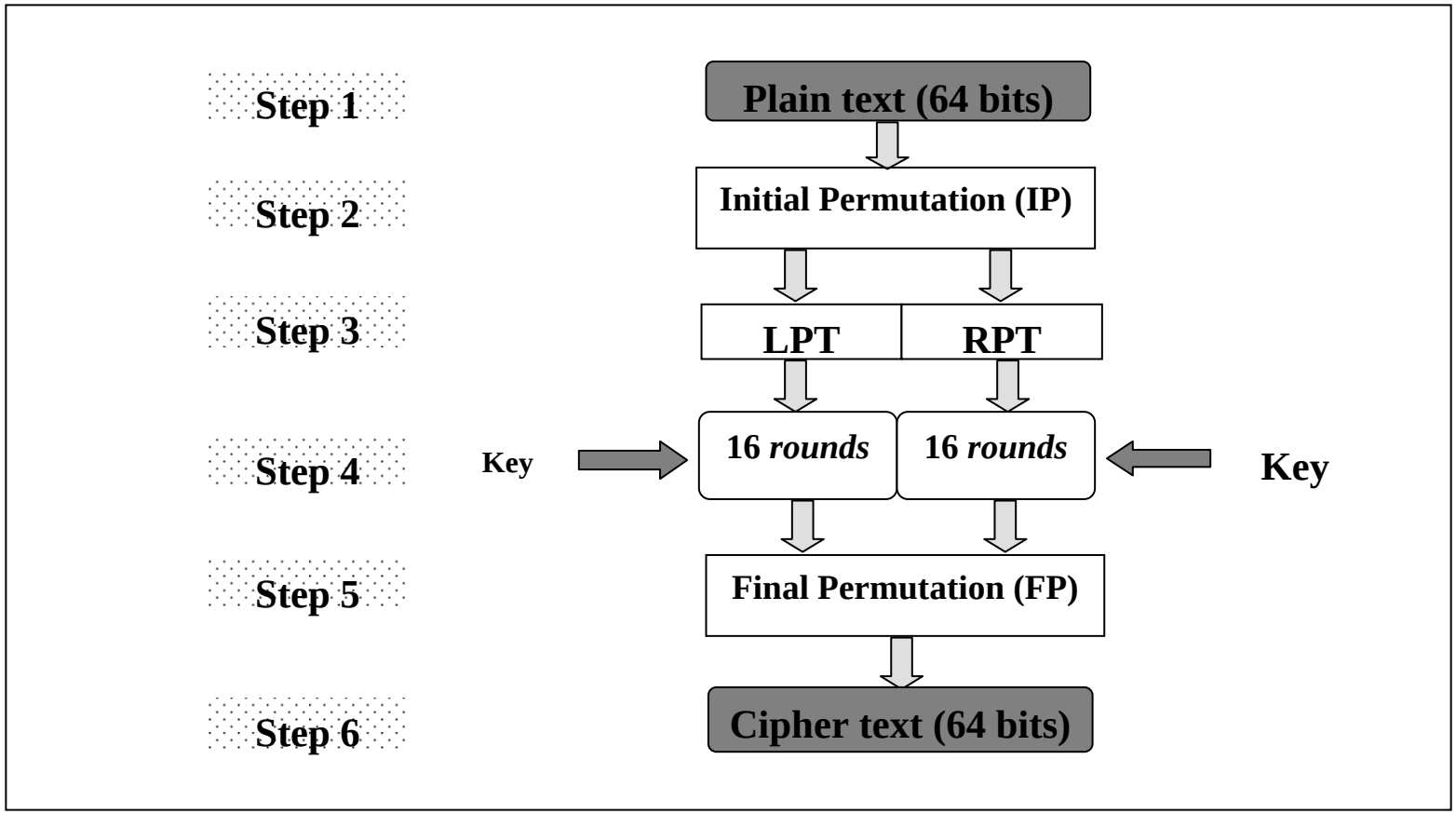

Fig 3.19

Details of One Round in DES

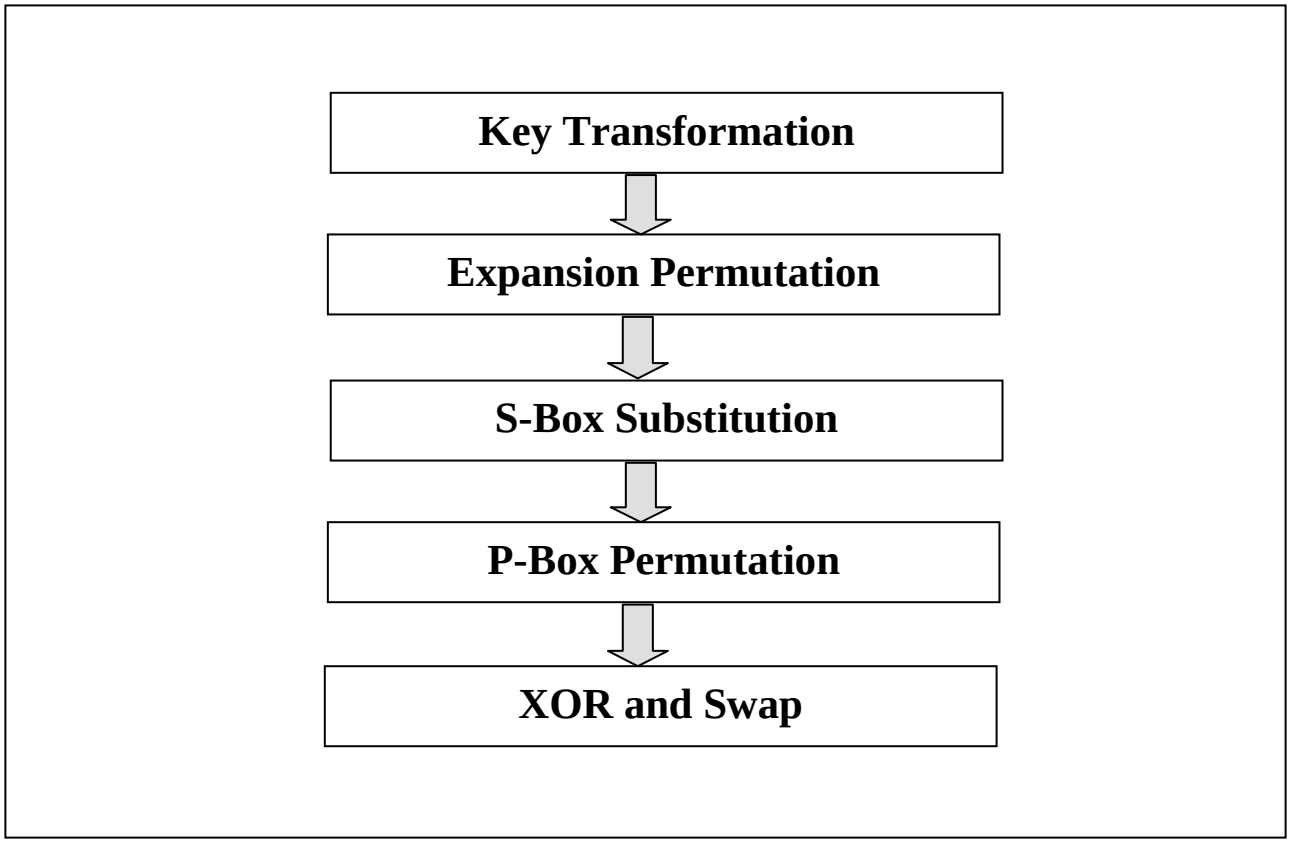

Fig 3.22

Modified Versions of DES

- Double DES: Perform DES twice with two different keys
- Triple DES with Three Different Keys
- Triple DES with Two Different Keys

Double DES Encryption

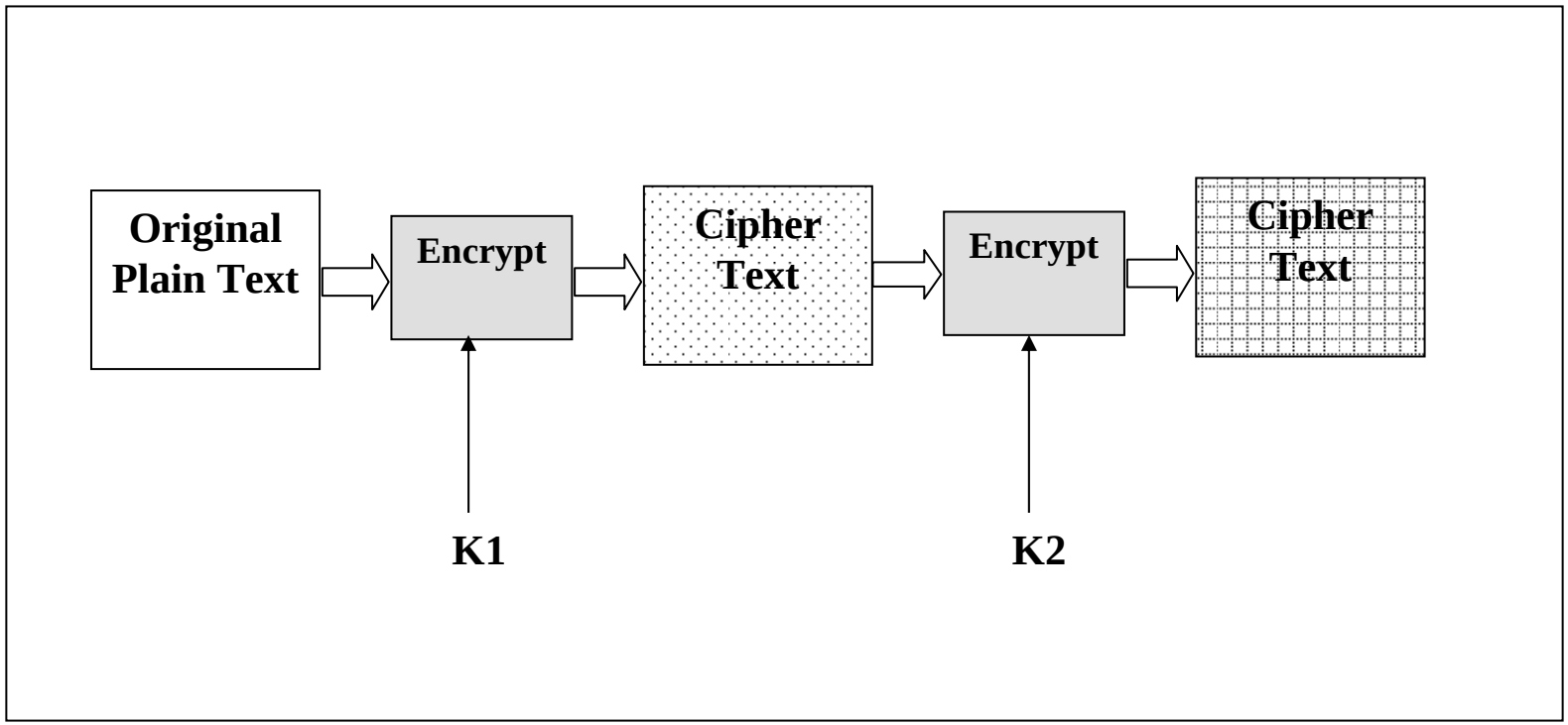

Fig 3.36

Double DES Decryption

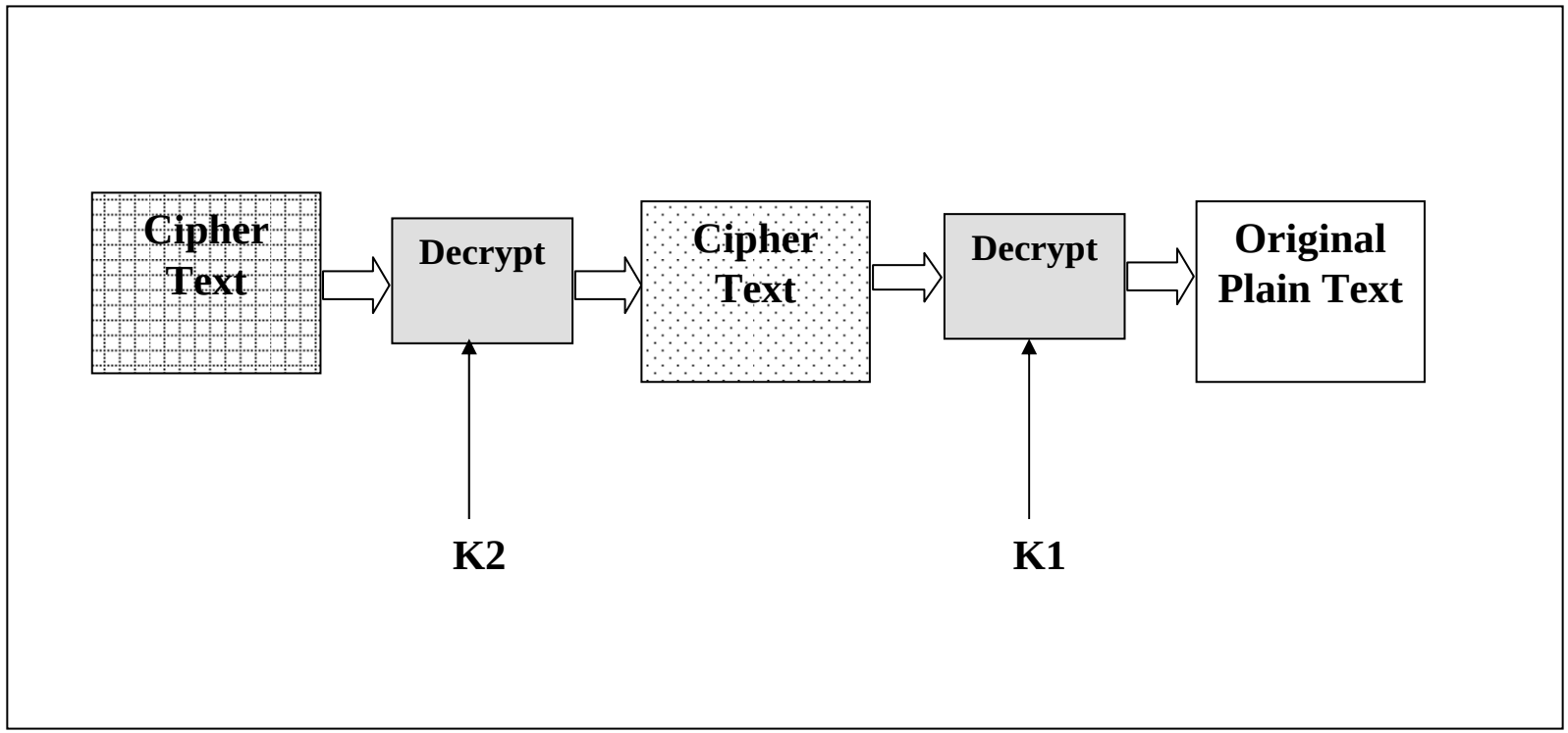

Fig 3.37

Double DES Mathematically Expressed

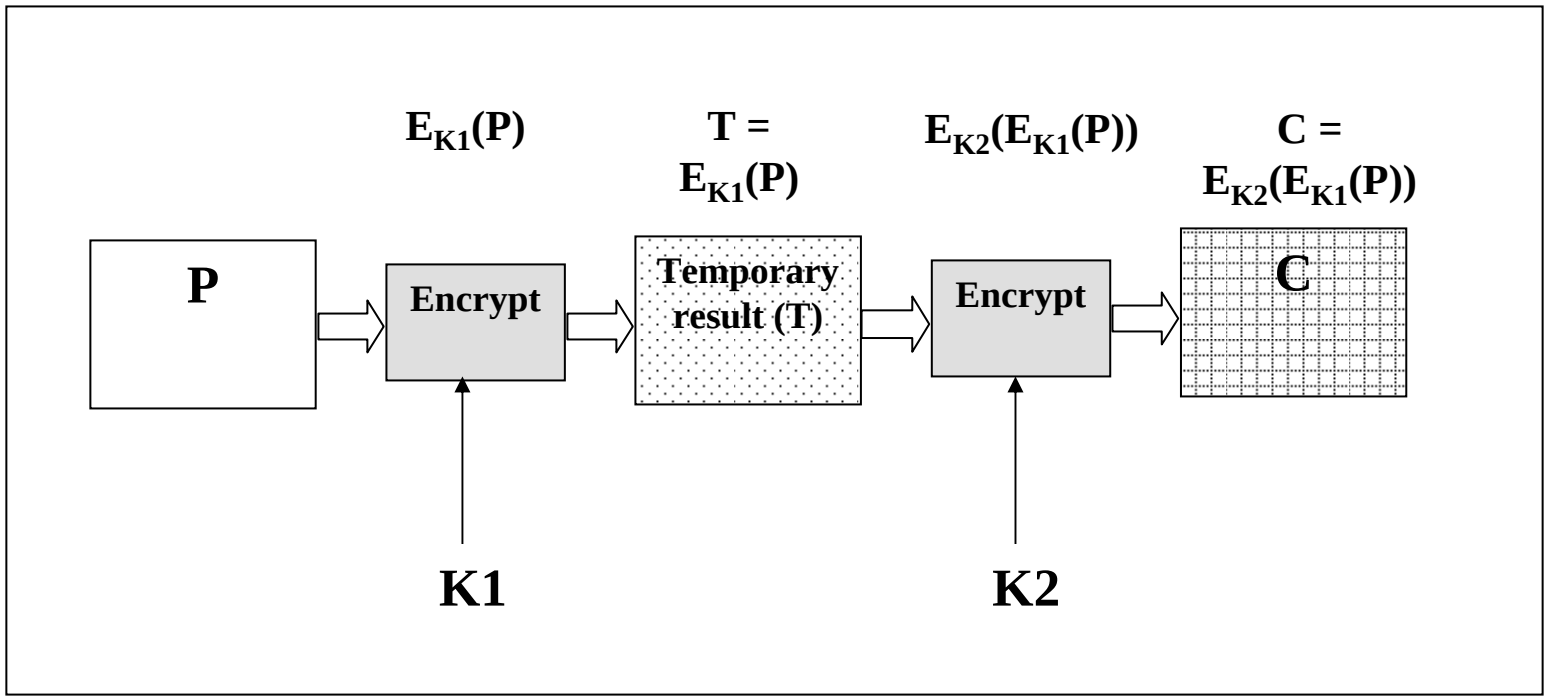

Fig 3.38

Triple DES

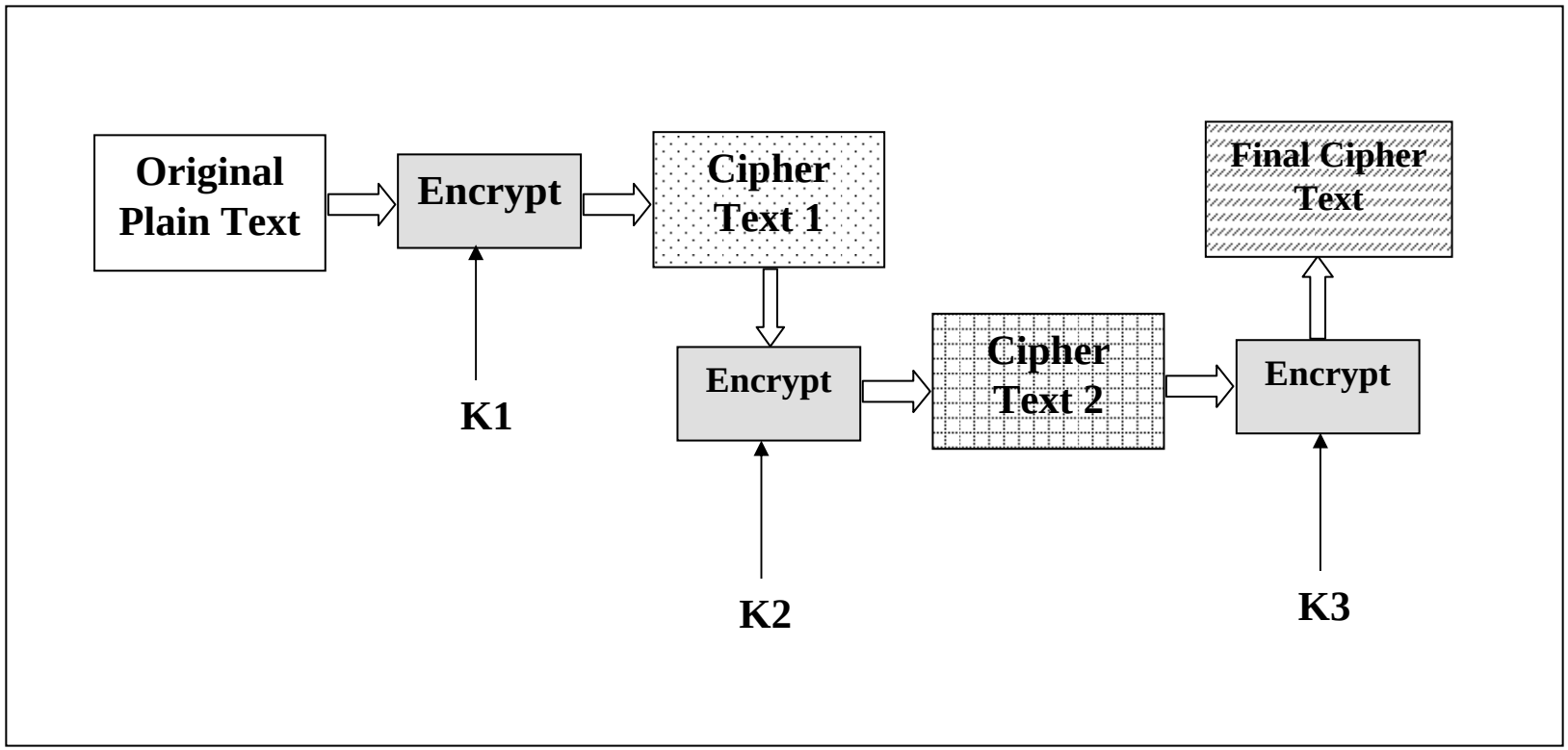

Fig 3.41

Triple DES with Two Keys

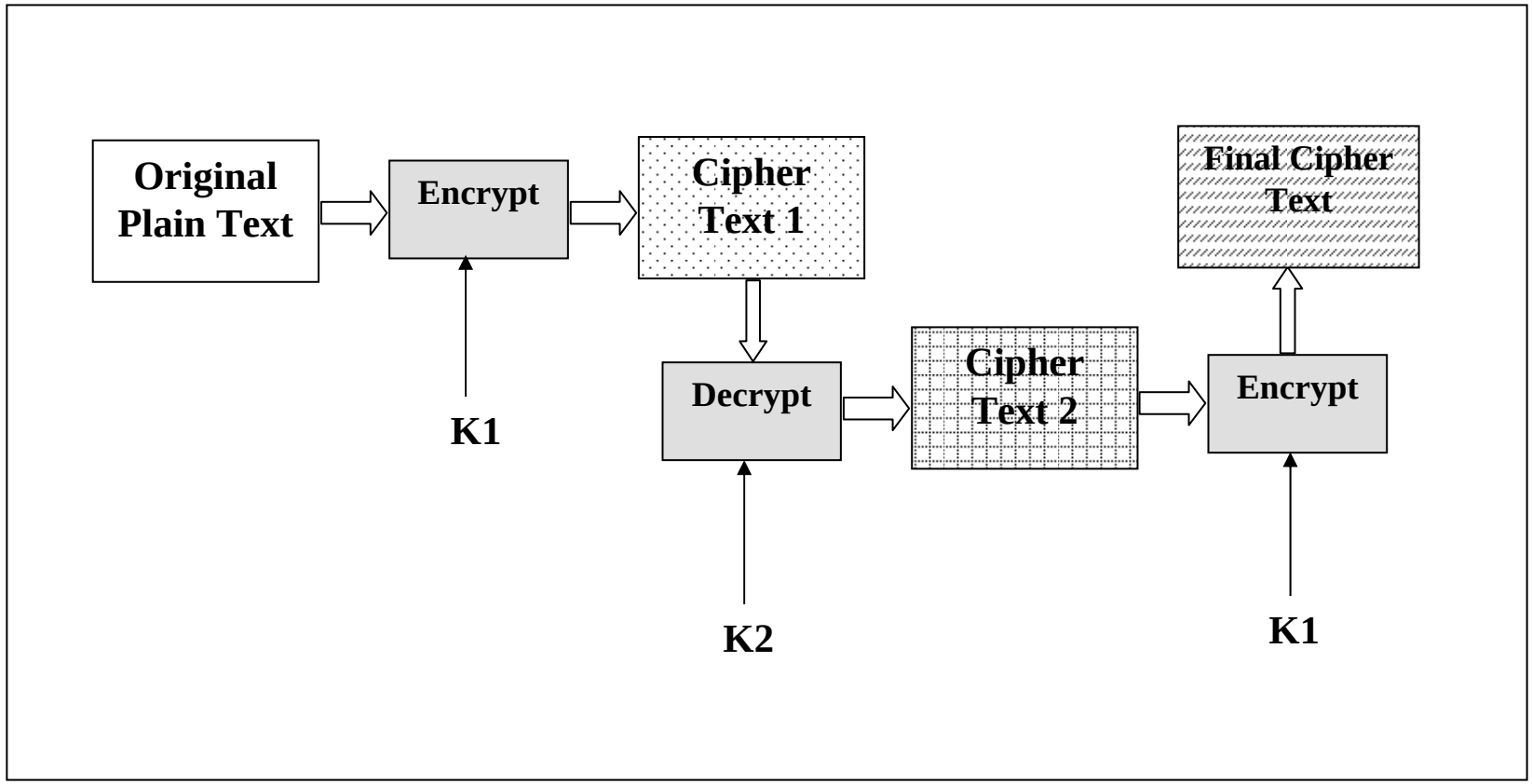

Fig 3.42

Broad Level Steps in IDEA

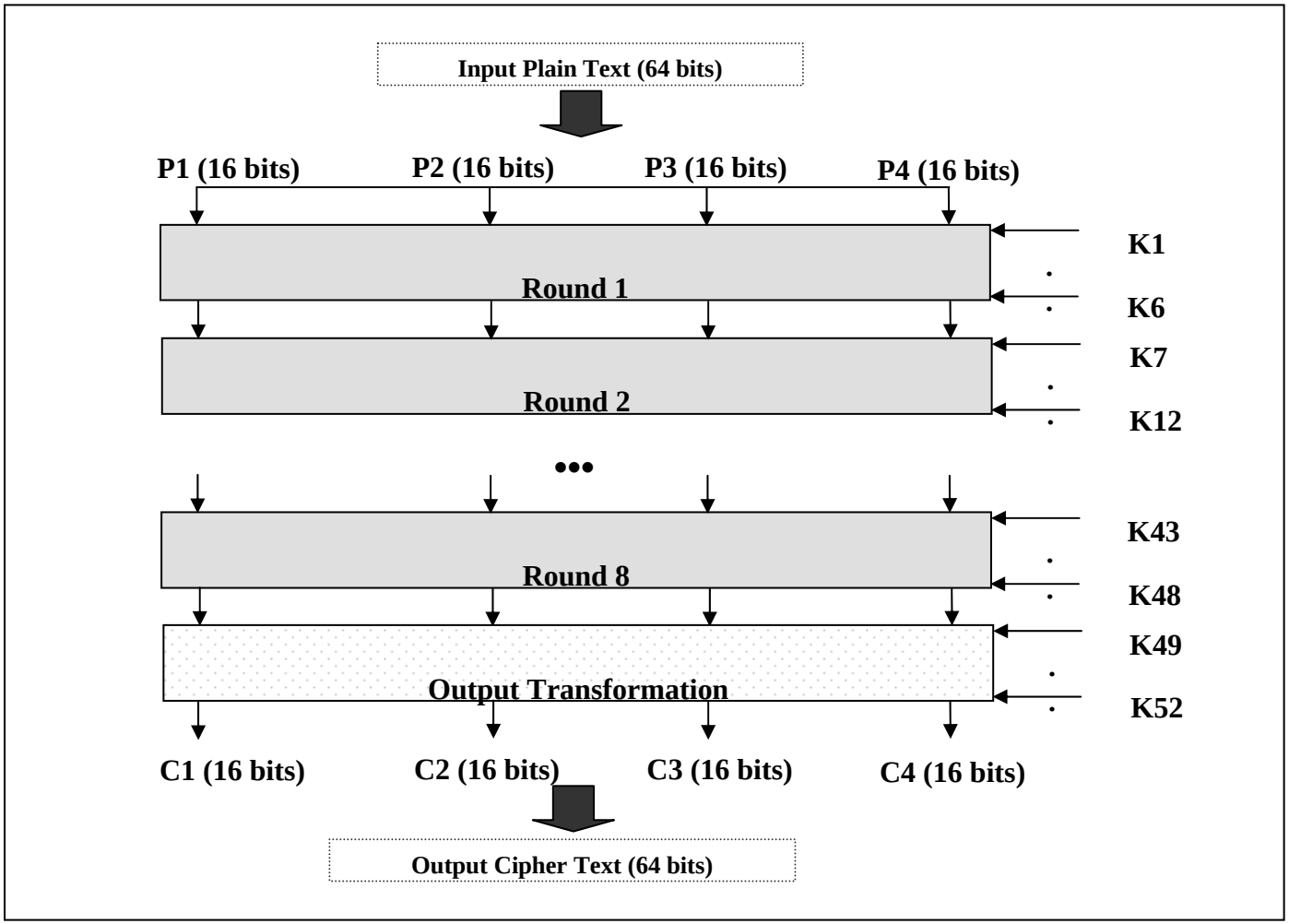

Fig 3.44

Encryption using RC5

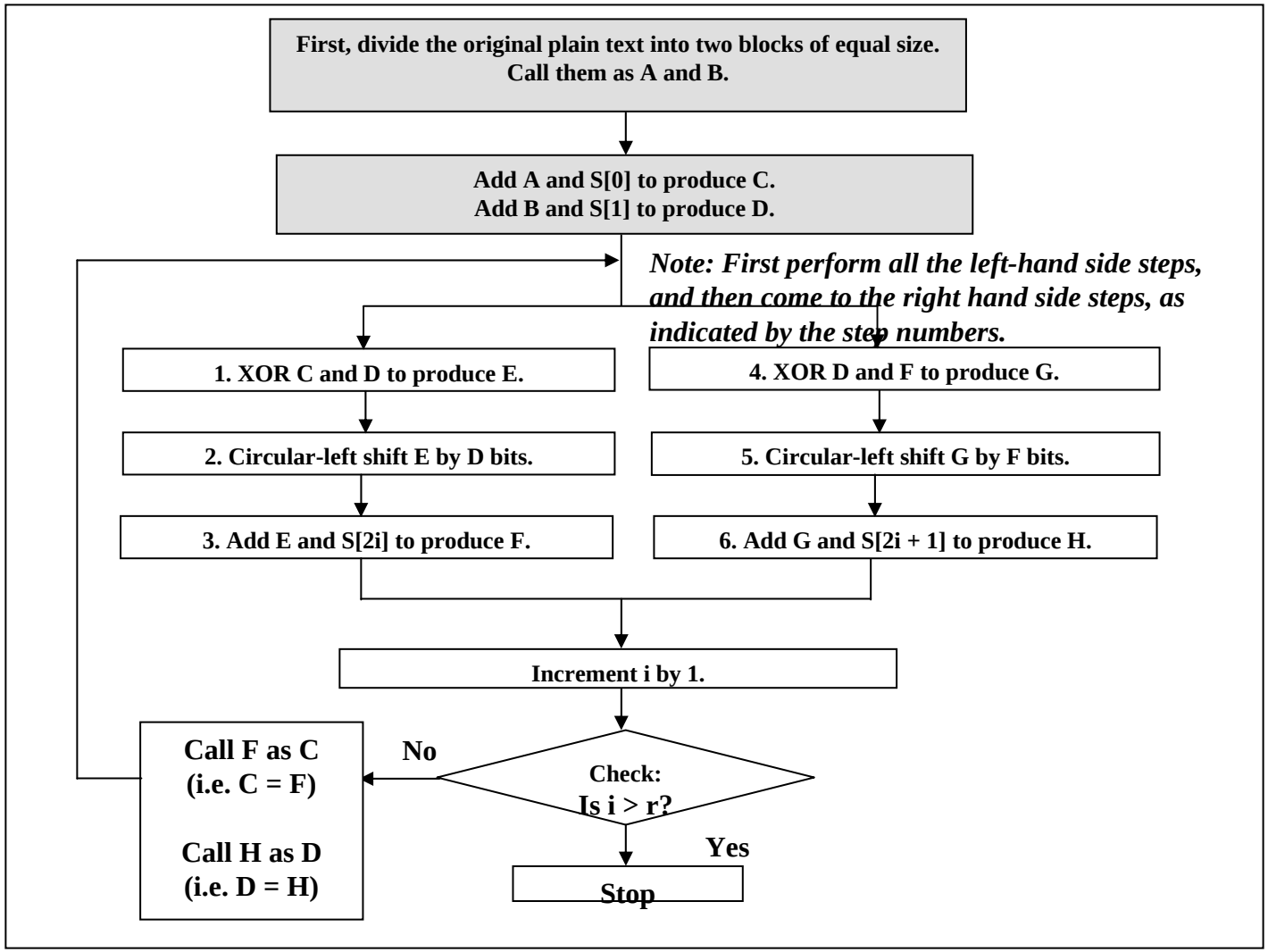

Fig 3.54

RC5 Encryption

```
A = A + S[0]
B = B + S[1]

For i = 1 to r
      A = ((A XOR B) <<< B) + S[2i]
      B = ((B XOR A) <<< A) + S[2i + 1]
Next i
```

Fig 3.63

RC5 Decryption

For i = r to 1 step –1 (i.e. decrement i each time by 1)
B = ((B – S[2i + 1]) >>> A) XOR A
A = ((A – S[2i]) >>> B) XOR B
Next i

B = B – S[1]
A = A – S[0]

Fig 3.64

Blowfish

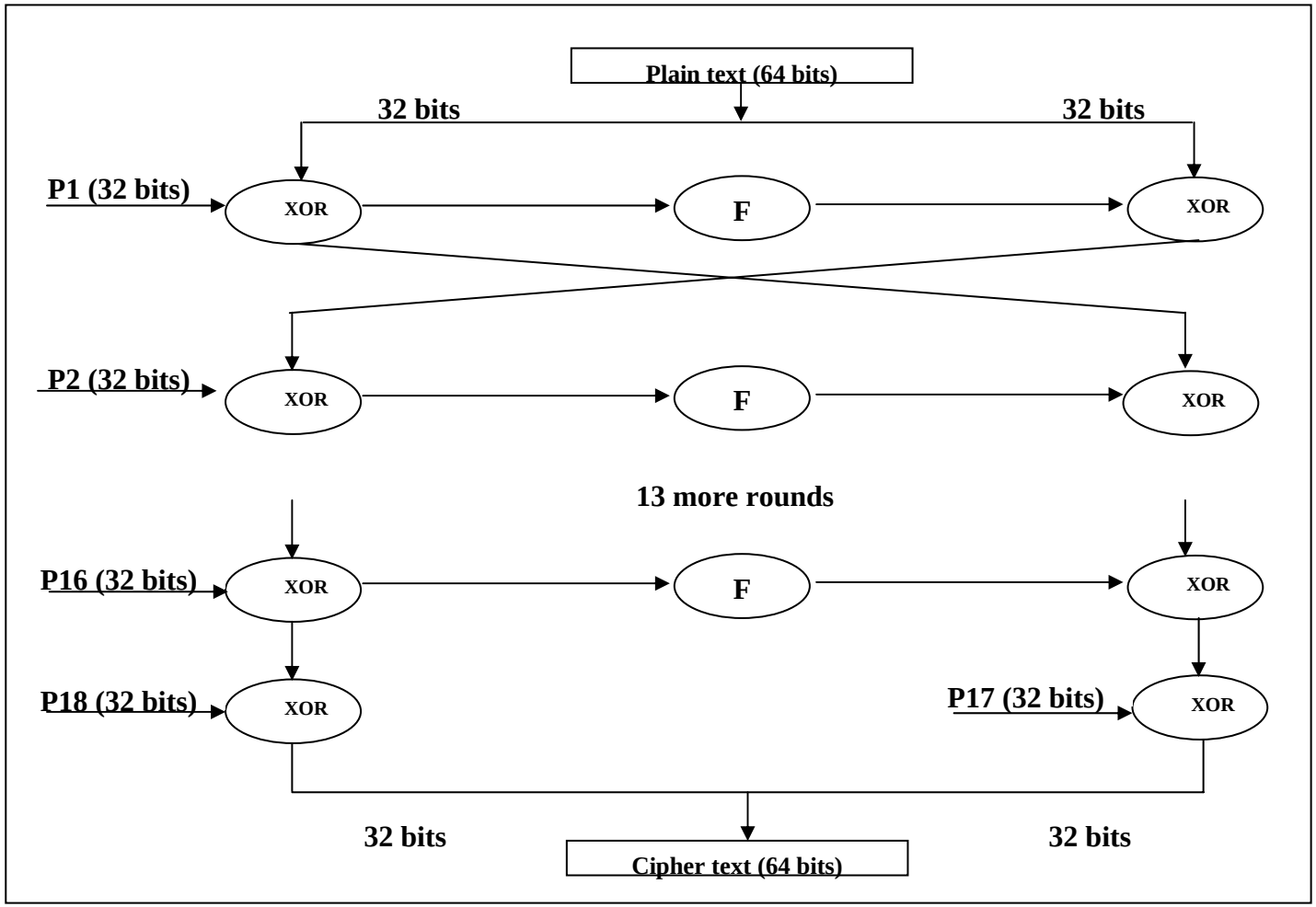

Fig 3.69

Rijndael (AES)

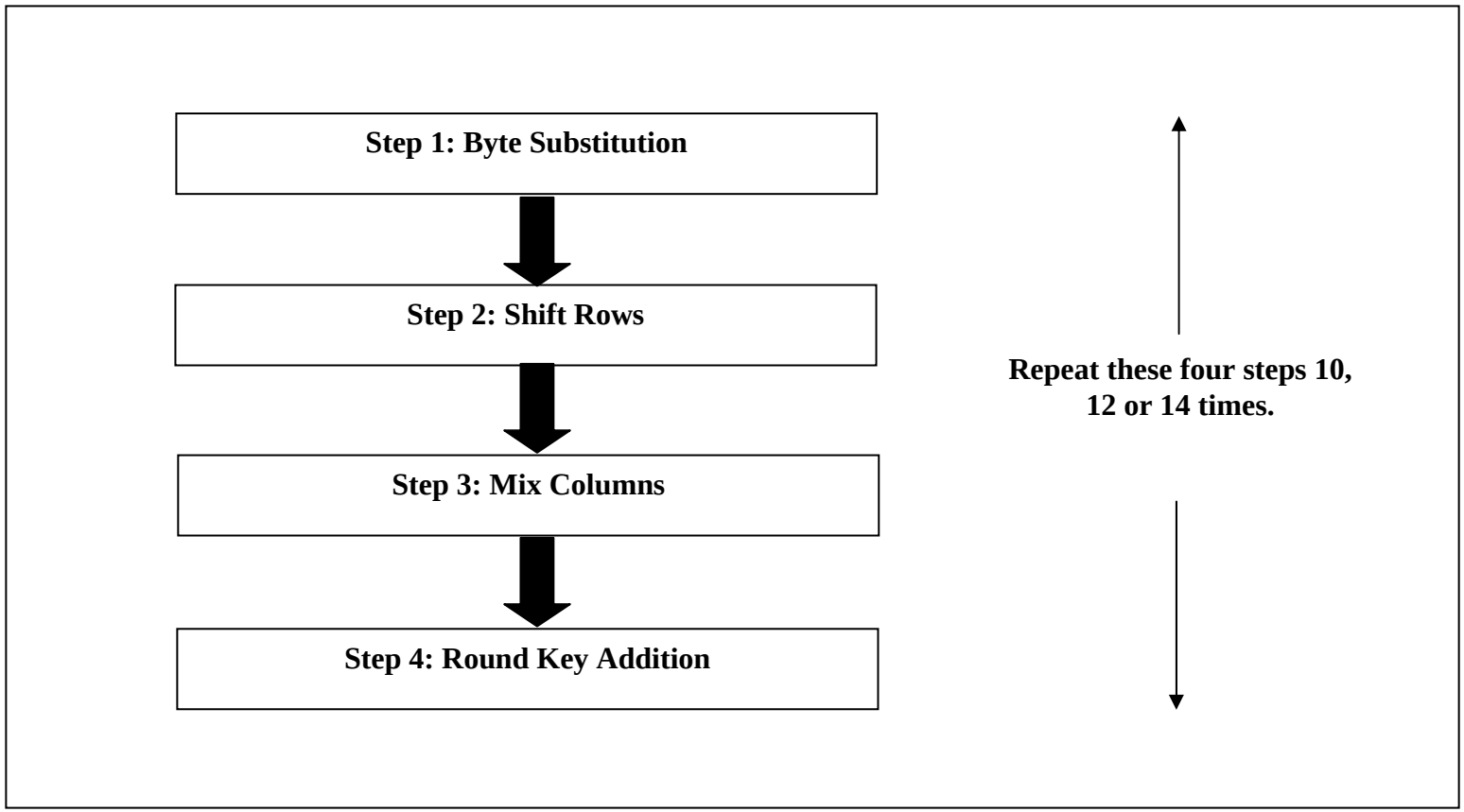

Fig 3.71